



BARLEY

Parish Council

‘Content, at the foot of Pendle’

Information Technology (IT) POLICY

1. Purpose

Barley Parish Council recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications.

This policy outlines the principles and procedures for the use, management, and security of IT systems, devices, and data within the Parish Council. It aims to ensure that technology is used responsibly, securely, and in compliance with legal and regulatory requirements.

2. Scope

This policy applies to all individuals who use the parish council’s IT resources, including computers, networks, software, devices, data, and email accounts.

The Council owns one dedicated personal computer which is held by the Clerk / RFO and has access to the dedicated council e-mail address. It is solely used for Council business.

Members are not issued with any IT devices. All formal communications are channelled through the Clerk/RFO, and occasionally the Chair, using this computer which has “cloud” storage support allowing users to access some data from other devices.

3. IT Governance

The Clerk is responsible for day-to-day IT management and liaising with external IT providers.

The Council will ensure appropriate budget provision for IT maintenance, upgrades, and cybersecurity.

All IT purchases must be approved by the Council and comply with procurement procedures.

4. Acceptable Use of IT resources and email

Council IT systems and devices must be used only for official Council business.

Personal use of Council devices is discouraged and must not compromise security or data integrity.

Users must not install unauthorised software or access inappropriate content.

All communications via Council email or social media must be professional and in line with Council values.

5. Data Protection and Privacy

All personal data will be handled in accordance with the GDPR and Data Protection Act 2018.

The Clerk is the designated Data Protection Officer and responsible for ensuring compliance.

Personal data must be stored securely and only accessed by authorised personnel.

Data breaches must be reported immediately to the Clerk and documented.

All sensitive and confidential parish council data should be stored and transmitted securely using approved methods. Regular data backups should be performed to prevent data loss, and secure data destruction methods should be used when necessary.

6. Email and Communication

The email accounts (clerk@barleyparish.uk) must be used for all official correspondence.

Emails and correspondence must be archived and retained in accordance with the document retention policy, typically retaining routine emails for 6–12 months and important correspondence for 1–6 years or longer, depending on content. Documents relating to significant decisions should be kept longer or permanently. All data must be held securely, preferably on official council-provided email systems rather than personal accounts.

Councillors are encouraged not use personal email accounts for Council business.

Users should be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

7. Website and Social Media

The Chairman and Councillor Grimshaw are responsible for maintaining the Council website and ensuring content is accurate and up to date.

Social media posts must be approved by the Clerk or Chair and reflect Council decisions and policies. *For more information see Barley PC Social Media Policy 2025.*

Comments and messages received via social media are discouraged as these can be easily missed and may not be responded to. Residents are encouraged to email the Clerk.

8. Security and Access Control

All devices must be password-protected and updated regularly.

Access to sensitive data and systems must be restricted to authorised users.

Remote access must be secured via VPN or encrypted connections.

Anti-virus and firewall protection must be maintained on all Council devices.

9. Backups and Disaster Recovery

Regular backups of Council data must be performed and stored securely.

A disaster recovery plan must be maintained to ensure continuity of operations in the event of IT failure, data loss or theft of the computer. 15GB of key information is be stored on the Google cloud and other information is stored on USB drives or memory cards.

10. Mobile Devices

The only mobile devices the Council own are tablets for issuing parking charge notices.

These should be stored safely and securely and kept charged as they may be required at short notice. No Council or private information should be stored on these devices.

11. Reporting and Enforcement

All suspected security breaches, incidents or IT issues should be reported immediately to the Clerk and IT Administrator Lead Councillor Grimshaw for investigation and resolution. Report any email-related security incidents or breaches to the IT administrator immediately.

12. Review and Updates

This policy will be reviewed every three years or sooner if required to ensure its relevance and effectiveness. Updates may be made to address any changes in legislation, emerging technology, security measures or Council operations.

All staff and councillors are responsible for the safety and security of the parish council's IT and email systems. By adhering to this IT and Email Policy, Barley Parish Council aims to create a secure and efficient IT environment that supports its mission and goals.

Any written concerns, complaints or compliments regarding this policy should be submitted to the Parish Clerk at clerk@barleyparish.uk

Status

Version	Date	Review Status
1.0	13 May 2026	Council Approved
2.0		